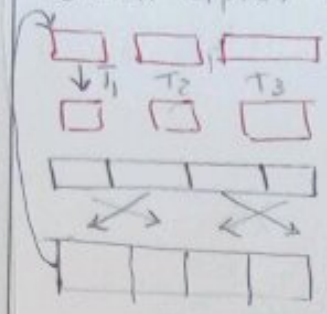
29/3/2017 الأربعاء د. رسيم محاضرة [4]

| | | | |
|---|---|---|---|
| Crypto | Block Cipher (symmetric key<br>  <br> | $K_s[m(i) \oplus r(i)] = C_i$<br>$C_i, r(i)$<br>CBC mode | $C_1 = K_s[m_1 + r_1]$<br>$C_1, r_1$<br>$C_2 = K_s[m_2 \oplus C_1]$<br>$C_2$<br>$C_3 = K_s[m_3 \oplus C_2]$<br>$C_3$ |
| Network | DES<br>56 bit | AES 128 bit | |

* تصنيفها إلى Public/Private Encryption ⟸ Authentication و privacy يسمح بـ
* الـ RSA Algorithm مطلوب
* الـ Hashing
* الـ Authentication من خلال الـ Hashing يسمى Digital Signature
* ~~الباقي من الربع - واجع الـ slides~~

Securing e-mail Slide 8.56, 5.58 --- All of it!

Securing TCP connection --- All of it!

الربع الـ PGP من الـ pdf المرقم بـ 736 صفحة